What is claimed is:

1. A method for incorporating confidentiality protection in a message transmitted between a user equipment and a network element in a communication network, wherein the message requires a sender identification and the sender of the message is one of the user equipment and the network element, the method comprising the steps of:

(a) assigning a temporary identity index for the sender of the message at each of the user equipment and the network element including performing an algorithm for generating the temporary identity index using public information which identifies the sender of the message as an input to the algorithm; and

(b) adding a header including the temporary identity index to the message to identify the sender of the message prior to transmission of the message between the user equipment and the network element.

2. The method of claim 1, wherein in said step (a), performing an algorithm includes performing a hash function using a private key and the public information as inputs to generate the temporary identity index.

3. The method of claim 2, wherein the public information used in said step (a) is an internet protocol multimedia public identity of the user equipment.

4. The method of claim 1, wherein the network element is located in a visiting network of the user equipment and said method further comprises the step of registering the user equipment with the visiting network before said step (a).

5. The method of claim 4, wherein said step of registering comprises sending, by the user equipment, a registration message to the network element, and retrieving, by the visiting network, the private key from a home network of the user equipment.

6. The method of claim 5, wherein the user equipment is authenticated after the network element retrieves the private key from the home network.

7. The method of claim 5, wherein the private key comprises one of a ciphering key and an integrity key.

8. The method of claim 5, further comprising the steps of determining an encryption algorithm and saving the private key, the encryption algorithm, and the temporary identity index in a memory in the visiting network.

9. The method of claim 1, wherein the message is a session initiation protocol message and the method further comprising the steps of:

generating the session initiation protocol message and encrypting the session initiation protocol message before performing said step (b); and

wherein said step (b) includes adding another line including the temporary identity index before the encrypted session initiation protocol message.

10. The method of claim 9, further comprising the steps of adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message.

11. The method of claim 9, wherein the session initiation protocol message includes a line including the request method that is encrypted with the session initiation protocol message.

12. The method of claim 9, wherein said step of adding another line comprises adding a call-info header and inserting the temporary identity index in the call-info header of the session initiation protocol message.

13. The method of claim 12, further comprising the step of performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code.

14. The method of claim 13, wherein said integrity algorithm comprises one of a message authentication code integrity algorithm and a modification detection code integrity algorithm.

15. The method of claim 14, wherein said integrity algorithm comprises MD5-MAC integrity algorithm.

16. The method of claim 9, further comprising the step of performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code.

17. The method of claim 16, wherein said integrity algorithm comprises one of a message authentication code integrity algorithm and a modification detection code integrity algorithm.

18. The method of claim 17, wherein said integrity algorithm comprises MD5-MAC integrity algorithm.

19. The method of claim 10, further comprising the step of encrypting a uniform resource identifier for the sender and adding the encrypted uniform resource identifier to the line including the request method.

20. The method of claim 19, wherein said step of adding another line comprises adding a call-info header and inserting the temporary identity index in the call-info header of the session initiation protocol message.

21. The method of claim 1, wherein said user equipment is a mobile phone.

22. The method of claim 1, wherein the algorithm is known to both the user equipment and the network element and said step (a) includes separately performing the algorithm at each of the user equipment and the network element.

23. The method of claim 1, wherein said step (a) includes performing the algorithm at the communication network and assigning the temporary identity index to the user equipment and the network element.

24. A system for performing confidentiality protection in a message transmitted between a user equipment and a network element in a communication network, wherein the message requires sender identification the sender of the message is one of the user equipment and the network element, said system comprising:

means for assigning a temporary identity index for the sender of the message at each of the user equipment and the network element including means for performing an algorithm for generating the temporary identity index using public information which identifies the sender as an input; and

means for adding a header including the temporary identity index to the message to identify the sender of the message prior to transmission of the message between the user equipment and the network element.

25. The system of claim 24, wherein said means for performing an algorithm includes means for performing a hash function using a private key and the public information for generating the temporary identity index.

26. The system of claim 25, wherein the public information is an internet protocol multimedia public identity of the sender.

27. The system of claim 24, wherein the communication network is a visiting network for the user equipment and the system further comprises means for registering the user equipment with the visiting network.

28. The system of claim 27, wherein said means for registering comprises means for sending a registration message from the user equipment to the visiting network, and means for retrieving the private key from a home network of the user equipment.

29. The system of claim 28, wherein said means for registering further comprises means for authenticating the user equipment.

30. The system of claim 28, wherein the private key comprises one of a ciphering key and an integrity key.

31. The system of claim 28, further comprising means for determining an encryption algorithm and wherein said visiting network comprises a memory for storing the private key, the encryption algorithm, and the temporary identity index.

32. The system of claim 24, wherein the message is a session initiation protocol message and said system further comprises:

means for generating the session initiation protocol message and encrypting the session initiation protocol message; and

wherein said means for adding a header including the temporary identity index includes means for adding another line including the temporary identity index before the encrypted session initiation protocol message.

33. The system of claim 32, further comprising means for adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message.

34. The system of claim 32, wherein the session initiation message includes a line including a request method that is encrypted with the session initiation protocol message by said means for generating and encrypting .

35. The system of claim 32, wherein said means for adding another line comprises means for adding a call-info header and inserting the temporary identity index in the call-info header of the session initiation protocol message.

36. The system of claim 35, further comprising means for performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code.

37. The system of claim 36, wherein said integrity algorithm comprises one of a message authentication code integrity algorithm and a modification detection code integrity algorithm.

38. The system of claim 37, wherein said integrity algorithm comprises MD5-MAC.

39. The system of claim 32, further comprising means for performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code.

40. The system of claim 39, wherein said integrity algorithm comprises one of a message authentication code integrity algorithm and a modification detection code integrity algorithm.

41. The system of claim 40, wherein said integrity algorithm comprises MD5-MAC.

42. The system of claim 33, further comprising means for encrypting a uniform resource identifier of the sender and means for adding the encrypted uniform resource identifier to the line including the request method.

43. The system of claim 42, wherein said means for adding another line comprises means for adding a call-info header and inserting the temporary identity index in the call-info header of the session initiation protocol message.

44. The system of claim 24, wherein said user equipment is a mobile phone.

45. The method of claim 24, wherein the algorithm is known to both the user equipment and the network element and said means for assigning includes means for separately performing the algorithm at each of the user equipment and the network element.

46. The method of claim 24, wherein said means for assigning includes means for performing the algorithm at the communication network and assigning the temporary identity index to the user equipment and the network element.

47. A computer-readable memory storing computer executable instructions for providing confidentiality protection to a message transmitted between a user equipment and a network element in a communication network, wherein the message requires sender identification and the sender of the message is one of the user equipment and the network element, said computer-readable memory comprising:

computer executable instructions for assigning a temporary identity index for the sender of the message at each of the user equipment and the network element including computer instructions for generating the temporary identity index by performing an algorithm using public information which identifies the sender of the message as an input; and

computer executable instructions for adding a header including the temporary identity index to the message to identify the sender of the message prior to transmission of the message between the user equipment and the communication network.

48. The memory of claim 47, wherein said computer-executable instructions for generating the temporary identity index include computer-executable instructions for performing a hash function using a private key and the public information for generating the temporary identity index.

49. The memory of claim 47, wherein the network element is located in a visiting network of the user equipment and the memory further comprises computer-executable instructions for registering the user equipment with the communication network.

50. The memory of claim 49, wherein said computer-executable instructions for registering comprises computer-executable instructions for sending a registration message from the user equipment to the network element.

51. The memory of claim 50, wherein the private key comprises one of a ciphering key and an integrity key.

52. The memory of claim 47, wherein the message is a session initiation protocol message and said memory further comprises:

computer-executable instructions for generating the session initiation protocol message and encrypting the session initiation protocol message before transmitting the message; and

wherein said computer-executable instructions for adding a header including the temporary identity index include computer-executable instructions for adding another line including the temporary identity index before the encrypted session initiation protocol message.

53. The memory of claim 52, further comprising computer executable instructions for adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message.

54. The memory of claim 52, further comprising computer executable instructions for adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message that is encrypted with the session initiation protocol message.

55. The memory of claim 52, wherein said computer-executable instructions for adding another line comprise computer-executable instructions for adding a call-info header and inserting the temporary identity index in the call-info header of the session initiation protocol message.

56. The memory of claim 55, further comprising computer-executable instructions for performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code.

57. The memory of claim 56, wherein said integrity algorithm comprises one of a message authentication code integrity algorithm and a modification detection code integrity algorithm.

58. The memory of claim 56, wherein said integrity algorithm comprises MD5-MAC.

59. The memory of claim 53, further comprising computer-executable instructions for encrypting a uniform resource identifier of the sender and for adding the encrypted uniform resource identifier to the line including the request method.

60. The memory of claim 59, wherein said computer-executable instructions for adding another line comprises computer-executable instructions for adding a call-info header

and inserting the temporary identity index in the call-info header of the session initiation protocol message.

61. The memory of claim 47, wherein said user equipment is a mobile phone.

62. The memory of claim 47, wherein the algorithm is known to both the user equipment and the network element and said computer instructions for generating include computer instructions for separately performing the algorithm at each of the user equipment and the network element.

63. The memory of claim 47, wherein said computer instructions for assigning include computer instructions for performing the algorithm at the communication network and assigning the temporary identity index to the user equipment and the network element.

64. A user equipment device for providing confidentiality protection to a message transmitted from the user equipment to a network element in a communication network, wherein the message requires sender identification, said user equipment device comprising:

means for assigning a temporary identity index for the user equipment; and

means for adding a header including the temporary identity index to the message to identify the user equipment as the sender of the message prior to transmission of the message between the user equipment and the communication network.

65. The device of claim 64, wherein said means for assigning includes means for generating the temporary identity index by performing an algorithm using public information which identifies the user equipment as the sender of the message as an input.

66. The device of claim 65, wherein said means for generating the temporary identity index include means for performing a hash function using a private key and the public information for generating the temporary identity index.

67. The device of claim 64, wherein the message is a session initiation protocol message and said device further comprises:

means for generating the session initiation protocol message and encrypting the session initiation protocol message before transmitting the message; and

wherein said means for adding a header including the temporary identity index include means for adding another line including the temporary identity index before the encrypted session initiation protocol message.

68. The device of claim 67, further comprising means for adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message.

69. The device of claim 67, further comprising means for adding a line before the encrypted session initiation protocol message including a request method of the session initiation protocol message that is encrypted with the session initiation protocol message.

70. The device of claim 67, wherein said means for adding another line comprise means for adding a call-info header and inserting the temporary identity index in the call-info header of the session initiation protocol message.

71. The device of claim 70, further comprising means for performing an integrity algorithm for the entire session initiation protocol message to calculate a code and adding an integrity header to the session initiation protocol message indicating the code.

72. The device of claim 69, further comprising means for encrypting a uniform resource identifier of the user equipment and for adding the encrypted uniform resource identifier to the line including the request method.

73. The device of claim 64, wherein said user equipment device is a mobile phone.

74. The device of claim 64, wherein said means for assigning include means for receiving the temporary identity index from the communication network and assigning the temporary identity index to the user equipment.